AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
[SUBJECT PREMISES] at 320 SE 10th St.
North Bend, WA 98045

Case No. MJ20-416

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
The SUBJECT PREMISES as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2252 (a)(2)	Receipt or Distribution of Child Pornography
Title 18, U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

✓ See attached Affidavit continued on the attached sheet

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Kevin Tilley
Applicant's signature

Special Agent Kevin Tilley, FBI
Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 07/13/2020

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Chief Magistrate Judge
Printed name and title

USAO: 2020R00338

ATTACHMENT A

(SUBJECT PREMISES)

The physical address of the SUBJECT PREMISES is 320 SE 10th St., North Bend, WA 98045, and is more fully described as a property containing a two-story, single-family home with an attached two-car garage and brown/gray color siding with white trim. There are stairs leading up to the front door of the residence.

The search is to include all rooms, persons, garages, vehicles, or outbuildings located on the SUBJECT PREMISES, as well as any digital device(s) or other electronic storage media found therein or thereon.

ATTACHMENT B

(PROPERTY TO BE SEIZED)

Evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), as follows:

a. Items, records, or information[1] relating to visual depictions of minors engaged in sexually explicit conduct;

b. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

c. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

d. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;

e. Items, records, or information related to communications with or about minors;

f. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;

g. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence,

[1] As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

purchase or lease agreements, diaries, statements, identification documents, address books, telephone directories, and keys;

h. Items, records, or information concerning the ownership or use of computer equipment found in the SUBJECT PREMISES or on the SUBJECT PERSON, including, but not limited to, sales receipts, bills for internet access, handwritten notes, and computer manuals;

i. Any digital devices or other electronic storage media[2]and/or their components including:

   i. any digital device or other electronic storage media capable of being used to commit, further, or store evidence, fruits, or instrumentalities of the offenses listed above;

   ii. any magnetic, electronic or optical storage device capable of storing data, including thumb drives, SD cards, or external hard drives;

   iii. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

   iv. any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

j. For any digital device or other electronic storage media whose seizure is otherwise authorized by this warrant, and any digital device or other electronic storage media that contains or in which is stored records or information that is otherwise called for by this warrant:

   i. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

[2] The term "digital devices" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "electronic storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

vi. evidence of the times the digital device or other electronic storage media was used;

vii. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

viii. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

ix. records of or information about the Internet Protocol used by the digital device or other electronic storage media;

x. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

xi. contextual information necessary to understand the evidence described in this attachment.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence,

fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Kevin Tilley, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Special Agent in Charge in Seattle, Washington. I have been an Agent with the FBI since November 2018. As part of my daily duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code §§ 2251(a), 2252A, 2422, and 2423. I specialize in the investigation of child pornography, including the transmission, possession and production of child pornography, exploitation of children on the internet, and other federal criminal activity. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. During my career as an FBI special agent, I have participated in numerous child pornography investigations. In addition, I have received training from the FBI and other institutions regarding computer related child pornography. I have received training in several P2P file sharing networks and training to use a law enforcement versions of those programs. I attended an investigations training program where I received training on a specific P2P file sharing network that is the subject of this affidavit. At that training, I learned how to use a law enforcement version of the Network P2P file sharing program. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures. I have received training regarding Internet crimes and child exploitation investigations. I have also participated in the execution of search warrants

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

involving investigations of child exploitation and/or child pornography offenses. I am a member of the Seattle Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for the following location and persons:

(1) The premises located at 320 SE 10th Street, North Bend, WA 98045 (hereinafter the "SUBJECT PREMISES"), further described in Attachment A, which is incorporated herein by reference; and

3. As set forth below, there is probable cause to believe that someone at the SUBJECT PREMISES has used a digital device to access the internet and distribute visual depictions of minors engaged in sexually explicit conduct. I therefore believe the SUBJECT PREMISES will contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography)(hereinafter the "TARGET OFFENSES"). I seek authorization to search and seize the items specified in Attachment B, which is incorporated herein by reference.

4. The information in this affidavit is based upon the investigation I have conducted in this case, my conversations with other law enforcement officers who have engaged in various aspects of this investigation, and my review of reports written by other law enforcement officers involved in this investigation. Because this affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are sufficient to establish probable cause to support the issuance

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of the requested warrants. When the statements of others are set forth in this affidavit, they are set forth in substance and in part.

PEER-TO-PEER (P2P) FILE SHARING

5. Peer to peer (P2P) file sharing is a method of communication available to internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the internet. There are multiple types of P2P file sharing networks on the internet. To connect to a particular P2P file sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the internet. A particular P2P file sharing network may have many different P2P client software programs that allow access to that particular P2P file sharing network. Additionally, a particular P2P client software program may be able to access multiple P2P file sharing networks. These P2P client software share common protocols for network access and file sharing. The user interface, features, and configurations may vary between clients and versions of the same client.

6. In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.

7. Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

8. Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

upon the P2P client software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

9. Typically, a setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. In some clients, individual files can also be shared.

10. Typically, a setting controls whether or not files are made available for distribution to other P2P clients.

11. Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of the file segments on the network for distribution.

12. Typically, files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. This client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same files are used during this process.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

13. P2P file sharing networks, including the BitTorrent network, are frequently used to trade digital files of child pornography. These files include both images and movie files.

14. The BitTorrent network is a very popular and publicly available P2P sharing network. Most computers that are part of this network are referred to as "peers." The terms "peers" and "clients" can be used interchangeably when referring to the BitTorrent network. A peer can simultaneously provide files to some peers while downloading files from other peers.

15. The BitTorrent network can be accessed by computers or mobile devices such as tablets and smart phones running many different client programs, some of which include the BitTorrent client program, uTorrent client program, and Vuze client program. These client programs are publicly available and free P2P client software programs that can be downloaded from the internet. There are also BitTorrent client programs that are not free. These BitTorrent client programs share common protocols for network access and file sharing. The user interfaces, features, and configuration may vary between clients and versions of the same client.

16. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files. Depending upon the BitTorrent client used, a user may have the ability to reconfigure some of those settings during installation or after installation has been completed. Typically, a setting establishes the location of one or more directories of folders whose contents (files) are made available to other BitTorrent network users to download.

17. In order to share a file or set of files on a BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share the file or set of files. A "Torrent" is typically a small file that describes the file(s) that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent client will have the ability to create a "Torrent" file. It is important to note that the "Torrent" file does not contain the actual file(s) being shared, but

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information about the file(s) described in the "Torrent," such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent." The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent," which include the SHA-1 hash value of each piece, the file size, and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate information about peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part, or all of the file(s) referenced in the "Torrent." It is important to note that the "Trackers" do not actually have the file(s) and are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

18. Once a "Torrent" is created, in order to share the file(s) referenced in the "Torrent" file, a user typically makes the "Torrent" available for other users, such as via websites on the Internet.

19. In order to locate "Torrent" files of interest, a typical user will use keyword searches within the BitTorrent network client itself or on websites hosting "Torrents." Once a "Torrent" file is located that meets the keyword search criteria, the user will download the "Torrent" file to their computer. Alternatively, a user can also search for and locate "magnet links," which is a link that enables the BitTorrent network client program itself to download the "Torrent" to the computer. In either case, a "Torrent" file is downloaded to the user's computer. The BitTorrent network client will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the remote peers/clients Internet Protocol (IP) addresses.

20. For example, a person interested in obtaining child pornographic images on the BitTorrent network would open the BitTorrent client application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." (It should be noted that this search term may not have been used in this investigation.) The results of the torrent search are typically returned to the user's computer by displaying them on the torrent hosting website. The hosting website will typically display information about the torrent, which can include the name of the torrent file, the name of the file(s) referenced in the torrent file, the file(s) size, and the "info hash" SHA-1 value of the torrent file. The user then selects a torrent of interest to download to their computer. Typically, the BitTorrent client program will then process the torrent file. The user selects from the results displayed the file(s) they want to download that were referenced in the torrent file. Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash Tables, Peer Exchange, and Local Peer Discovery), peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the torrent file available for sharing. The file(s) is then downloaded directly from the computer(s) sharing the file. Typically, once the BitTorrent network client has downloaded part of the file(s), it may immediately begin sharing the file with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 piece hash described in the torrent file. During the download process, a typical BitTorrent client program displays

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the Internet Protocol address of the peers/clients that appear to be sharing part or all of the file(s) referenced in the torrent file or other methods utilized by the BitTorrent network protocols. The downloaded file is then stored in the area previously designated by the user and/or the client program. The downloaded file(s), including the torrent file, will remain until moved or deleted.

21. Law Enforcement has created BitTorrent network client programs that obtain information from trackers about peers/clients recently reporting that they are involved in sharing digital files of known actual child pornography (based on the "info hash" SHA-1 hash value), which then allows the downloading of a file from a single IP address (as opposed to obtaining the file from multiple peers/clients on the network.) This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography on the BitTorrent network.

22. During the query and/or downloading process from a remote BitTorrent network client, certain information may be exchanged between the investigator's client and the remote client they are querying and/or downloading a file from. Such information could be 1) the remote client's IP address; 2) a confirmation from the remote client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the remote client program; and 3) the remote client program and version. This information may remain on the remote client's computer system for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

PROBABLE CAUSE

23. SA Arbuthnot-Stohl is a Special Agent with the FBI and has been so employed for approximately 15 years. She is currently assigned to the Seattle Division, Seattle Headquarter City of the FBI. She is a law enforcement officer of the United States, within the meaning of Title 18, United States Code, Section 2510(7), who is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516. In her capacity as a Special Agent for the Federal Bureau of Investigation, she is responsible for conducting federal and international investigations relating to crimes involving the sexual exploitation of children, including investigations related to online child exploitation. Included in these are laws relating to the unlawful production, importation, advertising, receipt, attempted receipt, possession, and distribution of child pornography, as outlined in Title 18, United States Code. She graduated from the FBI academy in 2010 and has received basic, advanced, and on-the-job training in the investigation of cases involving the sexual exploitation of children. She currently specializes in the investigation of child pornography, including the transmission, possession and production of child pornography, exploitation of children on the internet, and other federal criminal activity. She has received training in the area of child pornography and child exploitation and has had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256 in all forms of media including computer media. During her career as a FBI special agent, she has participated in numerous child pornography investigations. In addition, she has received training from the FBI and other institutions regarding computer related child pornography. She has specialized training in the use of law enforcement software designed to identify and apprehend users of P2P file sharing networks engaged in the trafficking of child pornography. She has conducted several investigations, obtained search warrants, made arrests, and obtained convictions based on P2P investigations. In April of 2019, SA Arbuthnot-Stohl completed an ICAC sponsored training in the BitTorrent (P2P) file sharing program.

24. In addition to the training on P2P file sharing I have received, I spoke with SA Arbuthnot-Stohl regarding the operation of BitTorrent as well as the information related to the BitTorrent user that is described below.

25. In March and April of 2020, while acting in an undercover capacity, SA Arbuthnot-Stohl utilized an automated law enforcement version of a publicly available

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Internet based peer to peer (P2P) file sharing program, known as BitTorrent, to monitor for P2P users possessing and distributing child pornography image and video files. BitTorrent Torrential Downpour, described below, is similar to BitTorrent except that it seeks out a specific torrent file (info Hash) from an IP address law enforcement is investigating, this is known as a single source download. The law enforcement version of BitTorrent will make repeated attempts to contact the subject IP address and download additional parts of the file. These repeated attempts can sometimes transpire over a period of several days. If a suspected child pornography file is large in size, such as a high definition video or a large image file set (image file sets are files containing numerous single image files stored within one or more separate folders), the law enforcement version of BitTorrent, due to system constraints, sometimes fails to download the entire file but is successful in downloading a number of the designated parts of the file. When this occurs with a video file, the downloaded file parts are often still viewable as short video segments and it is still possible to establish that the video file contains child pornography. When this occurs with large image file sets, the downloaded file parts are often individually viewable images, which can be reviewed to establish that the image file set contains child pornography.

26. Between March 27 and April 5, 2020, SA Arbuthnot-Stohl used the automated law enforcement version of BitTorrent to establish multiple single source connections with IP address 73.239.94.211 (the "SUBJECT IP ADDRESS") and to successfully download multiple files of child pornography. I describe five of the video files I have viewed below, some of which were complete and some of which were only partial:

File 1

This video begins by showing two prepubescent females facing the camera and in bathing suits. As the video progresses, a fully clothed adult male appears, and all three are shown in the nude. The adult male then engages in multiple sexual acts with one of the child victims. These include the child victim performing oral sex on the adult male and the adult male engaging in penetrative vaginal sexual intercourse with the child victim. Based on her stature, absence of visible pubic

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

hair, lack of apparent muscular and breast development, and youthful appearance, I estimate the child victim who is sexually abused by the adult male is between 7 and 10 years old.

File 2

This video begins by showing a nude adult male and a nude prepubescent female. The child victim is engaging in oral sex with the adult male. As the video progresses, the adult male is observed rubbing his penis against the child victim's chest. Soon after, the child victim is observed masturbating while the adult male is inserting his penis into her anus. The video ends with the adult male ejaculating onto the child victim. Based on her small stature, the absences of any visible pubic hair, lack of apparent muscular, and youthful appearance, I estimate the child victim is between 7 and 10 years old.

File 3

This video begins by showing two prepubescent males under a blanket. As the video progresses, the blanket is taken off by an individual who is off camera and the child victims are observed fully nude. The camera zooms in on the child victims' penises. Later in the video, one of the child victims is observed masturbating while the other is playing on a computer. One of the child victims is then observed engaging in oral sex with the other child victim. Throughout the video, it appears the child victims are talking to an unknown individual off camera. Based on their stature, absence of visible pubic hair, lack of apparent muscular, and youthful appearances, I estimate the child victims to be between 10 and 12 years old.

File 4

This video begins by showing a prepubescent female completely nude and on her knees engaging in oral sex with an adult male. The child victim continues engaging in oral sex until the man ejaculates. The video then changes, and the child victim is observed on a bed and completely nude. The child victim is manipulating her breasts with her hand. She is then observed masturbating with a sex toy. As the video progresses, the child victim is observed engaging in oral sex with another adult male. Later in the video, the adult male is observed anally raping the child victim with his penis and finger until ejaculation. During the middle part of the video, two prepubescent females are observed completely nude standing by a shower. As the video progresses, the original child victim is observed getting undressed and on her knees. An adult male is observed fully nude and instructing the child victim what to do. As the video progresses, at the 55:50 mark, the child victim is observed with her wrists bound and a collar around her neck. She is engaging in oral sex with an adult male. She is then observed with her

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ankles and knees bound while lying on a bed. An adult male is observed next to her. The camera is focused on the child victim's anus and vagina. The video cuts out and the child victim is observed engaging in oral sex with an adult male. The child victim is then observed manipulating her vagina with her fingers. The adult male is observed anally raping the child victim. The video ends with the child victim engaging in oral sex with the adult male. Based on her stature, absence of visible pubic hair, lack of apparent muscular and breast development, and youthful appearance, I estimate the child victim is between 8 and 10 years old.

File 5

This video begins by showing a prepubescent female sitting in a park. The video cuts out and the child victim is observed fully nude sitting on top of a bike. The child victim is observed rubbing her vagina on the seat and looking at the camera. The video cuts out again and the child victim is observed placing her vagina on the handlebars and rubbing her vagina against the handle bars as apparent masturbation. Based on her stature, absence of visible pubic hair, lack of apparent muscular and breast development, and youthful appearance, I estimate the child victim is between 9 and 11 years old.

27. A query of a publicly available database revealed the SUBJECT IP ADDRESS belonged to Comcast Communications.

28. In response to administrative summons seeking subscriber information for the SUBJECT IP ADDRESS, Comcast Communications reported that during the date and time of the downloads described above, the SUBJECT IP ADDRESS was assigned to S.W. with a service address at the SUBJECT PREMISES.

29. Washington State Department of License information shows that P.W., K.W. and J.A.G. list the SUBJECT PREMISES as their address on valid Washington driver licenses and/or identification cards issued to them. Based on my investigation to date, including a review of other law enforcement and public information databases, it appears that a fourth adult, J.S.G., may also reside at the SUBJECT PREMISES. J.A.G. and J.S.G. are brothers and the adult children of K.W.

30. From my investigation, S.W., the subscriber of the Comcast account to which the SUBJECT IP ADDRESS was assigned during the relevant period, appears to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

be a male relative of P.W. It does not appear that S.W. resides at the SUBJECT PREMISES, however.

31. As outlined above, multiple sources of information indicate that someone residing at the SUBJECT PREMISES used a computer connected to the internet via the SUBJECT IP ADDRESS to share files depicting minors engage in sexually explicit conduct. Though S.W. was the subscriber of this IP address during the relevant time, the more important factor is the physical location of that IP address at that time, which was the SUBJECT PREMISES. Based on my knowledge, training, and experience, and the experience of other law enforcement officers, I know that it is common for multiple individuals and computers within a residence to share Internet access. I therefore believe evidence of that crime will be found in the SUBJECT PREMISES.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

32. As part of my training and experience, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

33. Based on my training and experience, that cellular phones (referred to herein generally as "smart phones") have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

another. Many people generally carry their smart phone on their person; recent investigations in this District have resulted in the discovery of child pornography files on smart phones which were carried on an individual's person at the time the phones were seized.

34. As set forth above and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes that might be at the SUBJECT PREMISES or on the SUBJECT PERSON, in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store child pornography in electronic form. The ability to store child pornography in electronic form makes digital devices an ideal repository for child pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

35. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is collected, distributed, and produced. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these images was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation would follow the same paths. More recently, through the use of computers and the Internet, distributors of child

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

pornography use membership based/subscription based websites to conduct business, allowing them to remain relatively anonymous.

36. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography as described in this Affidavit.

37. Producers of child pornography can now produce both still and moving images directly from the average video or digital camera. These still and/or moving images are then uploaded from the camera to the computer, either by attaching the camera to the computer through a USB cable or similar device, or by ejecting the camera memory card from the camera and inserting it into a card reader. Once uploaded to the computer, the images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to those by which a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. Producers of child pornography can also use a scanner to transfer printed photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

38. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers, including ISPs, allow email service between subscribers and sometimes between their own subscribers and those of other networks.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In addition, these service providers act as a gateway for their subscribers to the Internet. Having said that, however, this application does not seek to reach any host computers.

39. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography, and (ii) websites that offer child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the distributors/recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the distributor/recipient.

40. The computer's capability to store visual depictions in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 2 terabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage elsewhere. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

41. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly. They also may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an Internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.]

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

42. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

43. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the person who used a computer to connect to the internet with the SUBJECT IP ADDRESS and share child pornography likely has a sexualized interest in children and depictions of children and that evidence of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

child pornography is likely to be found at the SUBJECT PREMISES or a person residing at the SUBJECT PREMISES.

FRUITS, EVIDENCE, AND INSTRUMENTALITIES INSIDE THE SUBJECT PREMISES AND ANY CLOSED CONTAINERS AND ELECTRONIC DEVICES FOUND THEREIN

44. As described above and in Attachment B, this application seeks permission to search for and seize items listed in Attachment B that might be found in the SUBJECT PREMISES or on a person residing at the SUBJECT PREMISES, in whatever form they are found. One form in which evidence, fruits, or instrumentalities might be found is data stored on a computer's hard drive or other digital device[1] or electronic storage media.[2]Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

45. Through my training and experience, and the information learned during the course of this investigation, I know that individuals who engage in child pornography offenses often keep physical evidence, fruits, and instrumentalities of their crimes inside their residences, including but not limited to, digital devices

46. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensic examiners, and my training and experience, I submit that if a digital

---

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

device or other electronic storage medium is found in the SUBJECT PREMISES or on a person residing at the SUBJECT PREMISES, there is probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES will be stored on those digital devices or other electronic storage media. As detailed above, my investigation shows someone used a computer at the SUBJECT PREMISES connected to the internet via the SUBJECT IP ADDRESS to share files of child pornography. There is, therefore, probable cause to believe that evidence, fruits, and instrumentalities, of the crimes under investigation exist and will be found on digital devices or other electronic storage media at the SUBJECT PREMISES or on a person at the SUBJECT PREMISES, for at least the following reasons:

a. Based my knowledge, training, and experience, I know that computer files or remnants of such files may be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, this information can sometimes be recovered months or years later with forensics tools. This is because when a person "deletes" a file on a computer, the data contained in the files does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in "swap" or "recovery" files.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what is has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. Digital storage devices may also be large in capacity, but small in physical size. Because those who are in possession of such devices also tend to keep them on their persons, especially when they may contain evidence of a crime. Digital storage devices may be smaller than a postal stamp in size, and thus they may easily be hidden in a person's pocket.

47. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on digital devices found in the SUBJECT PREMISES or on a person residing at the SUBJECT PREMISES, because:

a. Data on the digital storage medium or digital devices can provide evidence of a file that was once on the digital storage medium or digital devices but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to further establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g. registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search of "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further computer and storage media activity can

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer activity associated with user accounts and electronic storage media that connected with the computer. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit the crime (e.g. Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper content, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing a user's intent.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. I know that when an individual uses a computer to store, receive, or distribute child pornography, the individual's computer or digital device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer or digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer or digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer or digital device used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of text discussions about the crime; and other records that indicate the nature of the offense.

48. *Necessity of seizing or copying entire computers or storage medium.* In most cases, a thorough search of a premises for information that might be stored on digital storage media or other digital devices often requires the seizure of the digital devices and digital storage media for later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic copy of the digital media's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

49. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all the necessary technical manuals and specialized equipment necessary to consult with computer personnel who have expertise in the type of computer, operating system, or software application being searched.

50. The analysis of computer systems and storage media often relies on rigorous procedures designed to maintain the integrity of the evidence and to recover "hidden," mislabeled, deceptively named, erased, compressed, encrypted or password-protected data, while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment such as a laboratory, is typically required to conduct such an analysis properly.

51. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impracticable to search for data during the execution of the physical search of the premises. The hard drives commonly included in desktop and laptop computers are capable of storing millions of pages of text.

52. A search of digital devices for evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents may recover evidence with carefully targeted searches to locate evidence without requirement of a manual search through unrelated materials that may be commingled with criminal evidence. Agents may be able to execute a "keyword" search that searches through the files stored in a digital device for special terms that appear only in the materials covered by the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

warrant. Or, agents may be able to locate the materials covered by looking for a particular directory or name. However, in other cases, such techniques may not yield the evidence described in the warrant. Individuals may mislabel or hide files and directories; encode communications to avoid using keywords; attempt to delete files to evade detection; or take other steps designed to hide information from law enforcement searches for information.

53. The search procedure of any digital device seized may include the following on-site techniques to seize the evidence authorized in Attachment B:

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or co-conspirators.

b. On-site copying and analysis of volatile memory, which is usually lost if a computer is powered down, and may contain information about how the computer is being used, by whom, when and may contain information about encryption, virtual machines, or stenography which will be lost if the computer is powered down.

c. On-site forensic imaging of any computers may be necessary for computers or devices that may be partially or fully encrypted in order to preserve unencrypted data that may, if not immediately imaged on-scene become encrypted and accordingly become unavailable for any examination.

54. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

55. Based on the information set forth herein, there is probable cause to search the above described SUBJECT PREMISES or on a person residing at the SUBJECT PREMISES, as further described in Attachment A, as well as on and in any digital device or other electronic storage media found at the SUBJECT PREMISES or on a person residing at the SUBJECT PREMISES, for evidence, fruits and instrumentalities, as further described in Attachment B, of the TARGET OFFENSES.

Kevin Tilley, Affiant
Special Agent, FBI

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit this 13th day of July, 2020.

HON. BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

(SUBJECT PREMISES)

The physical address of the SUBJECT PREMISES is 320 SE 10th St., North Bend, WA 98045, and is more fully described as a property containing a two-story, single-family home with an attached two-car garage and brown/gray color siding with white trim. There are stairs leading up to the front door of the residence.

The search is to include all rooms, persons, garages, vehicles, or outbuildings located on the SUBJECT PREMISES, as well as any digital device(s) or other electronic storage media found therein or thereon.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

(PROPERTY TO BE SEIZED)

Evidence, fruits, and instrumentalities of violations 18 U.S.C. §§ 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), as follows:

a. Items, records, or information[3] relating to visual depictions of minors engaged in sexually explicit conduct;

b. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

c. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

d. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;

e. Items, records, or information related to communications with or about minors;

f. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;

g. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence,

[3] As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

purchase or lease agreements, diaries, statements, identification documents, address books, telephone directories, and keys;

h. Items, records, or information concerning the ownership or use of computer equipment found in the SUBJECT PREMISES or on the SUBJECT PERSON, including, but not limited to, sales receipts, bills for internet access, handwritten notes, and computer manuals;

i. Any digital devices or other electronic storage media[4] and/or their components including:

i. any digital device or other electronic storage media capable of being used to commit, further, or store evidence, fruits, or instrumentalities of the offenses listed above;

ii. any magnetic, electronic or optical storage device capable of storing data, including thumb drives, SD cards, or external hard drives;

iii. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

iv. any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

j. For any digital device or other electronic storage media whose seizure is otherwise authorized by this warrant, and any digital device or other electronic storage media that contains or in which is stored records or information that is otherwise called for by this warrant:

i. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry

---

[4] The term "digital devices" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "electronic storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the lack of such malicious software;

iv. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

v. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

vi. evidence of the times the digital device or other electronic storage media was used;

vii. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

viii. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

ix. records of or information about the Internet Protocol used by the digital device or other electronic storage media;

x. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

xi. contextual information necessary to understand the evidence described in this attachment.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970